CHAPTER ONE

1

Overview of Enterprise Risk Management

ERM INTRODUCTION

Enterprise risk management (ERM) includes the methods and processes used by organizations to minimize surprises and seize opportunities related to the achievement of their objectives.

ERM is an approach to aligning strategy, process, and knowledge in order to curtail surprises and losses as well as to capitalize on business opportunities. Many individuals associate risk with negative outcomes. However, there is a potential value component to risk assessment and management. Risk management is about balancing risk and reward. A well-designed risk management program encourages and allows an organization to take intelligent risks. It involves assessing quantitative factors and information as well as considering management experience and judgment. An effective risk management program entails balancing people and processes. Ultimately, an entity's risk profile

is affected by the actions and decisions of its board of directors, management, and employees.

One cannot talk about risk management without discussing risk assessment. The vast majority of organizations conduct some type of informal risk assessment process. As a result, these organizations have some form of risk management plan. This plan, in most cases, is not documented.

Initial introduction of formal risk assessment and risk management within an organization is critical to the ultimate success of the initiative. An entity must consider its culture and develop an approach that is most likely to result in success. The organization should take care not to overcomplicate or overwhelm individuals with technical terminology. Initial discussions should focus on the importance and the benefits of risk management. Employees should be encouraged to think and talk about the business and what could go wrong that might result in failure to achieve entity objectives and, as a result, have a negative effect on performance and/or perception.

Good risk management is essentially choice management. It is a continuous work in progress. An entity must identify risks and subsequently determine how it will address each one. The organization must decide the degree of risk it is willing to assume and address other identified risks, likely through mitigation. It is important to consider both tangible consequences, such as loss of revenue or drop in stock price, as well as intangible possibilities, such as public perception. Perception often is a major consideration in assessing positive or negative consequences. Organizations often evaluate risks in somewhat of a siloed process—considering the risk consequence to a single area of the business. Risks are inherently dynamic and interdependent. Consequences of unforeseen or unpredictable events typically affect multiple areas of a business. Therefore, aggregate entity consequences should be considered when conducting a risk assessment and designing a risk management program. Risks should not be separated into components and managed independently. Such an approach is rarely effective or successful. A holistic view of risk should be taken, including the contemplation of interdependencies.

Every organization is faced with uncertainty and risk. The challenge for management is to determine how much uncertainty to accept as it strives to improve stakeholder value.

Risk identification is a process designed to identify first both the strategic objectives and goals and then the potential internal and external events that can adversely affect the enterprise's ability to achieve those objectives and goals.

Each entity should strive to build an integrated risk organization. This would include three components: (1) centralized risk management reporting to the chief executive officer and the board of directors, (2) an integrated risk management strategy that takes a holistic view of all types of risk within the organization, and (3) integration of risk management into business processes.

It is not easy to accomplish these stated objectives. The method and processes for execution may vary significantly based on the size, structure, and culture of the organization. Each company must determine the most practical method of implementation. However, this integrated approach will allow risk management to become an offensive weapon for management rather than the more common defensive reaction to incident occurrence.

Organizations should take a proactive approach to optimizing their risk profiles. Minimal investment in risk assessment and subsequent risk management program development and implementation can improve efficiency and reduce losses.

GUIDANCE: HISTORY AND RELATIONSHIP

Due to the heightened scrutiny and concentration on risk and risk management, there is a great deal of guidance available. Prior to exploring ERM design and implementation details, it is beneficial to examine various frameworks and standards. There will be extensive reference to these guidance documents in this book. The frameworks and standards discussed here are not the only sources of information available. The publications presented are commonly referenced and have been suggested for use by many industry-specific organizations. Some of the guidance, by nature of the issuer, is intended primarily for auditor use; some is directed to management. Certain publications provide broad advice regarding risk management; other documents specifically concentrate on risks and controls over financial reporting. However, examination of all of the recommendations, regardless of the source or intended audience, is valuable when undertaking a risk management initiative.

In 1992, the Committee of Sponsoring Organizations (COSO) of the Treadway Commission first issued a conceptual framework entitled *Internal Control—Integrated Framework*. COSO originally was charged with studying and reporting on factors that can lead to fraudulent financial reporting. The COSO Framework was intended for broad use by any organization, and it provides evaluation tools that can be utilized for comprehensive evaluation of control

systems. This is evidenced in the general nature of the COSO definition of internal control:

> A process, affected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
>
> - Effectiveness and efficiency of operations
> - Reliability of financial reporting
> - Compliance with applicable laws and regulations

Subsequently, with the passage of the Sarbanes-Oxley Act (SOX) in 2002, the Securities and Exchange Commission (SEC) suggested management use of the COSO Framework specifically for the design, build, and/or analysis of internal control over financial reporting. Details of the components of the COSO Framework and its use in the risk management and risk assessment process are presented in Chapters 5 and 6.

SOX established the Public Company Accounting Oversight Board (PCAOB), a private, nonprofit corporation whose mission is to oversee the auditors of public companies. To date, the PCAOB has issued five auditing standards (ASs); the most recent is AS No. 5, *An Audit of Internal Control over Financial Reporting that Is Integrated with an Audit of Financial Statements*. This standard directs auditors to adopt a top-down risk-based approach to internal control and compliance during the audit process. It points auditors toward initial review of entity-level controls and emphasizes the significance of strength at this level. In addition, the standard reinforces the importance of auditor focus on high-risk areas and situations and provides auditor guidance regarding the confirmation of risk mitigation in those identified areas.

In 2004, COSO published the *ERM—Integrated Framework*. It was issued to assist organizations to identify, assess, and manage risk effectively. The document establishes key risk management principles, concepts, language, and guidance with a goal of aiding an entity in formally establishing or improving its risk management. Details of the components of the *Integrated Framework* and its use in the risk management and risk assessment process are presented in Chapter 4.

The Auditing Standards Board has issued several Statement of Auditing Standards (SASs), commonly referred to as the Risk Assessment SASs (SAS 104–111), that outline auditor requirements, including documentation specifically associated with risk assessment. This guidance includes auditor requirements

for understanding and documenting management's risk assessment process as well as documentation of the auditor's own risk assessment process as part of audit planning.

All of the standards and frameworks contain detailed guidance that is valuable to an entity when designing, building, and/or analyzing its internal control and risk management program. The remainder of the text refers to these documents extensively because of their definitions, concepts, and advice. Risk management involves risk assessment, which results in risk mitigation, which occurs through the existence or implementation of control activities. All of these are interrelated and defined as well as referenced in one or more of the documents mentioned.

ORGANIZATION VIEW

Figure 1.1 illustrates an organization view of risk management and its role and relationship to overall corporate governance and compliance. Each entity should seek to build its organizational structure to support a top-down approach that begins with consideration of overall corporate governance, progresses to risk management and assessment, and ultimately considers the achievement of all compliance requirements. SOX Section 404 compliance requirements created an inverted pyramid effect. Many organizations focus primarily on compliance and secondarily on risk management and governance. More recently, there has been emphasis from governing bodies, guidance, and standards regarding the appropriate top-down focus and process. Thus, entity attention has shifted in this direction.

Executive management in tandem with the board of directors should develop and document a strategy that outlines what the organization expects to accomplish—its goals—as well as the objectives it must achieve in order to realize the desired results. When determining a strategy, the board of directors and senior management may ask: How are we going to create value for our stakeholders? The answers manifest themselves in a strategic plan and associated objectives. *A clearly documented strategy and associated objectives are critical to the development of an effective ERM program.* An outline in these areas allows the organization to focus on opportunities presented in the strategic plan as well as to minimize the potential impact of threats. From a practical prospective, this may be a single-page document that outlines organization goals in terms of areas such as the customer, financial expectations, and products/services. The strategic plan, at the highest level, will aid in the

FIGURE 1.1 Organization View of Risk Management

facilitation of all future discussions regarding risk and risk mitigation. The organization should consider the strategy from a financial and an operational perspective. *The absence of a documented strategy and objectives, including related policies and job descriptions that outline overall expectations and define roles and responsibilities, significantly impairs an entity's ability to design and implement an effective ERM program.*

Once the entity has documented and can articulate its strategy and related objectives, it can then develop and implement an ERM program. Doing this includes performance of a risk assessment, which includes considering what could go wrong that might prohibit the entity from achieving its objectives. Therefore, it is extremely difficult, if not impossible, to execute this process effectively if the strategy and objectives are not defined initially.

Part of the risk assessment process should include consideration of entity compliance with all applicable laws and regulations.

Ultimately the entity will seek to mitigate identified risks through numerous forms of control activities.

ERM TODAY

Less than a decade ago, ERM was not a major focus for most organizations. Today, it is quickly ascending to the top of the agendas of senior executives and shareholders alike as corporate scandals and globalization challenge the status quo and regulators publish new or updated requirements.

ERM is a structured approach to aligning strategy, processes, people, technology, and knowledge to identify and manage uncertainties and risk. Providing a comprehensive, integrated framework that enables organizations to *proactively manage* business risk, ERM aids in the achievement of balance between business needs and risk thresholds to increase competitive advantage and shareholder value. ERM definitions tend to vary from source to source, but all contain common themes: a standard risk management process, an integrated view of risks, and a focus on relating risks to business objectives.

One would think that recent corporate scandals and fraud as well as provisions set by SOX would have spurred companies to assess and improve the management and mitigation of enterprise-wide risks. Despite the plethora of internal and/or external events that could expose an organization to serious risks, companies focus much more on measuring and monitoring financial performance than on proactively measuring, analyzing, and responding to and mitigating risks—threats that could negatively impact financial performance.

The majority of risk management experts agree that companies, for the most part, are not doing a good job of assessing and managing risk because they lack either the discipline for it or a mandate from executive management. However, risk management is rapidly becoming a major area of focus, and risk areas within each organization should be analyzed. A number of major drivers prompt the development of a formal enterprise risk framework, including:

- *Regulatory guidance.* Several recent SEC releases reference a risk-based approach to compliance. This focus serves as an excellent platform for the design and implementation of an enterprise-wide risk management program. The program does not have to be implemented throughout the entire organization concurrently but can be rolled out using a phased approach (e.g., business unit, geography, function, etc.).

- *Evolving roles of the audit committee and board of directors.* Since the passage of SOX, audit committee members and directors have increased responsibilities and greater accountability. This has prompted them to focus inquiries on the organization's plans for developing a formal risk management strategy and plan.
- *Risk assessment standards.* The SASs 104 through 111 (effective December 2006) and SAS 115 require the auditor, among many other items, to direct a significant amount of focus on understanding and documenting the entity and its environment, including internal control. The standards also emphasize the importance of the entity's risk assessment process and how it correlates to the entity's process of setting strategies and objectives and assessing related business risk.

Companies that assess risk, set risk thresholds, and actively monitor and manage their risk exposure within those thresholds are better able to predict future performance more accurately. They are also more likely to achieve higher performance and/or meet financial expectations because they are better able to potentially avoid large fluctuations in business and avoid the negative consequences of unmitigated risk events.

Although the percentage of organizations without a formal ERM program in place is declining, it is surprising how few organizations have such a program. Even if companies have a risk management program, often it is more informal in nature. This is shocking, given the amount of money that has been lost in the financial markets due to poor risk management and fraud.

Note: It is critical that any reader understand, prior to proceeding through this book, how the words "internal control" are used and their relationship to any discussion about risk management. First, any reference or use of the words "internal control" or "risk management" applies to *all* organizations, private or public, large or small, for-profit or nonprofit. The difference is in the design of the risk management program or system of internal control as appropriate for an individual entity and its specific structure and circumstances. This book often mentions controls and internal controls. Very simply put, controls mitigate risk. Finance and accounting professionals, due partially to the nature of our training, often immediately associate any reference or discussion of internal control with financial reporting and disclosure. However, the reader should bear in mind that the term "internal control" applies to any and all risk mitigation activity, regardless of the risk category. These controls exist in many different forms and activities within the structure and processes of each organization.

INCREASED PRESSURE TO MANAGE RISK

A number of prominent events stimulate a case for increased risk assessment and risk management programs, including:

- The recent financial crisis and the existence of volatile market conditions.
- A significant increase in identified major fraud incidents, such as the Madoff case, which resulted in millions of dollars in losses for individuals as well as a number of organizations.
- Accounting scandals, such as Enron and WorldCom, that caused a public loss of confidence in financial reporting.
- Increased regulatory pressure, including the passage of the Dodd-Frank Wall Street Reform and Consumer Protection Act in 2010 and SOX as well as the recent SEC concentration on review of risk information in annual quarterly and proxy filings.
- The recent focus of credit rating agencies on ERM processes.

The events listed provide additional incentive for organizations to consider either the enhancement or the development of a risk management program.

Although most of the events outlined have had a greater regulatory and financial impact on public organizations, these incidents definitely have affected private and nonprofit companies. This fact is evidenced by several occurrences. Several audit firms have migrated to one method of audit for all of their clients, regardless of their status, public or private. Therefore, the auditors are concentrating considerable effort understanding and documenting client internal control as well as their risk assessment process. Many financial institutions/lenders and granting agencies have begun requesting information regarding an entity's internal control. Moreover, many private entities' board of directors have begun to query management regarding risk management and internal control over financial reporting.

SAS 115 requires that if, during the course of the financial statement audit of a private company, the auditor identifies any significant deficiencies or material weaknesses in internal control over financial reporting, the auditor must report those identified deficiencies in writing (SAS 115 letter) to management and those charged with governance. This requirement further evidences the reason for the auditor attention on risk assessment and internal control over financial reporting as well as the increased pressure on private companies to concentrate additional effort in these areas.

ADDITIONAL EVIDENCE

Recently, in its reviews of regulatory filings, the SEC has been encouraging companies to provide more information regarding risks they face and dissuading the use of boilerplate language. In addition, the regulator has warned entities regarding its increased focus on risk disclosures. The SEC has stated that entities should refrain from "copying and pasting" risk disclosures from quarter to quarter. When commenting on recent reviews, the SEC has referred to disclosures as too broad and generic, and the regulator is demanding risk information that is specific to an organization including the board's role in risk oversight.

CFO Magazine lists these ten as the most frequently questioned issues in the SEC comments on companies' risk factors over the past two years:

1. Inadequate disclosure issues
2. Market for products and services
3. Reliance on suppliers, customers, governments
4. Going concern
5. Effects of regulatory changes
6. Legal exposures and reliance on legal positions
7. Ineffective internal or disclosure controls
8. Reliance on certain employees
9. Conflicts of interest/related party issues
10. History of operating losses[1]

The Corporate Executive Board's top ten high-risk areas of focus for 2010 cited by finance executives included:

1. Strategic change management
2. Capacity
3. Incentive plans
4. Human resources
5. Fraud
6. Innovation/research and development
7. Third-party relationships
8. Shared services
9. Inflation/Deflation
10. Tax management[2]

All of the summarized data listed should be considered by organizations, public or private, when conducting a risk assessment.

PERCEIVED BARRIERS TO RISK MANAGEMENT

Most organizations report competing priorities, insufficient resources, and lack of perceived value in addition to absence of board of director and/or senior leadership support for the initiative as major barriers to risk management program implementation. These companies often state that they feel overwhelmed by a daunting, lengthy process with which they have little familiarity. In addition, most individuals believe that the design and implementation of an ERM program is extremely costly. Based on this assumption, many organizations believe that they lack the financial resources to develop and sustain the program. In some cases, management and the board of directors are not aware that they are implicitly responsible for risk management within their organization.

BUILDING THE BUSINESS CASE FOR ERM: VALUE AND BENEFITS

All organizations face uncertainty. Uncertainty presents risk as well as opportunity.

A well-designed ERM solution will provide an entity with numerous tangible and intangible benefits.

The goal of every company is to maximize value for its shareholders. Value certainly can be created or deflated by business decisions made at the top, but it also can be created, preserved, or eroded by routine decisions that occur at every level within the organization. ERM supports value creation by helping management assess future events and respond in a manner that reduces the likelihood of outcomes that would lead to value erosion. Effective risk management supports the alignment of an entity's documented strategy and objectives with the risk management plan; it also facilitates communication of the strategy, objectives, and ERM plan throughout the organization. In addition, an effective ERM program fosters greater accountability, responsibility, and ownership for internal controls throughout the organization.

Successful long-term risk management enables the organization to anticipate risks resulting from opportunity, uncertainty, and hazards that can present occasions for either value enhancement (i.e., upside risk) or value erosion

(i.e., downside risk). ERM can aid in creating and/or preserving a company's value by dealing effectively with potential future events that create uncertainty. Analysis of upside risk can provide valuable insight that management can use to plan actions that will achieve positive gains. Defensively managing downside risk through policies, procedures, and systems may help prevent behaviors that could negatively impact company performance.

A functional approach to risk management often creates "silos" that can be difficult to manage across the enterprise. An integrated ERM framework allows for risks to be managed effectively across business units, functions, and business activities. Employees can be empowered to own and manage risks in their respective areas. This approach also increases risk transparency throughout the organization.

The real value of ERM surfaces when organizations look beyond assessing risk for the sole purpose of meeting minimum regulatory requirements. A comprehensive risk management plan presents a higher value proposition. The benefits of pursuing such a solution can be numerous. A few of the main benefits include:

- *Cost savings through an integrated approach to compliance.* Overlapping requirements and initiatives, which compete for company resources and management's attention, have prompted an increasing number of companies to develop a common framework for addressing all regulatory and management requirements. Such an integrated approach, including internal audit, regulatory compliance, and process improvement, can provide considerable savings over the cost of multiple stand-alone responses by providing greater operational efficiency. In addition, an integrated approach may assist in fostering greater accountability and ownership for internal controls throughout the organization.
- *Ability to assess current risk position and respond.* The absence of an ERM program makes it much more difficult for an organization to evaluate its risk position. Without this ability, an entity is disadvantaged. The existence of a formalized, documented risk assessment facilitates improved risk management and mitigation and enables the organization to better align strategy with acceptable levels of risk.
- *Improved proactive management.* The existence of an ERM program facilitates a proactive versus reactive approach. A well-developed plan can help a company's board and senior management team focus their efforts on strategic decision making rather than reacting to unexpected risks. Increasing management's focus on the future based on existing information and

analysis, rather than crisis management, can lead to improved decision making and a better competitive position for the company. Thus, operational surprises and losses are minimized. In addition, management response to challenges and opportunities is enhanced. ERM supports management decisions regarding activity such as product development, pricing, and acquisitions.

- *Optimized capital structure and allocation.* Improved estimation of a company's capital requirements is one of the most frequently cited benefits of ERM. A better understanding of risk across an organization leads to a more thorough understanding of what capital is required to support a given risk tolerance. ERM also leads to better capital allocation among business units. As risk management capabilities improve, a company can achieve a greater level of transparency, which helps boards and senior executives make more informed decisions about capital allocation as well as business mix, products, and future investments.

If effectively implemented, an ERM program can help an entity achieve its goals and potentially avoid surprises along the way while providing value to stakeholders.

KEYS TO SUCCESS

Successful ERM initiatives have several consistent themes. It is important to keep these general thoughts/concepts in mind when considering an ERM implementation.

- *Executive support is critical to the success of the initiative.* ERM should be incorporated into the culture and viewed as an important, company-wide strategic initiative. Support at the top is a necessity and should begin with the board of directors and extend to executives and senior management through to each employee at every level. Clear demonstration of support and expectations should be communicated, both initially and consistently at every appropriate opportunity. The tone-at-the-top sponsorship and testimony is especially important for establishing the appropriate internal environment, which is fundamental for the creation of a solid ERM program foundation.
- *The development of a risk intelligent culture is beneficial.* Historically, most small organizations have spent little, if any, time formally considering,

discussing, documenting, and/or analyzing risk. In order to navigate effectively and efficiently through the risk management process as well as obtain buy-in, both of which are critical to a successful initiative, the organization should seek to become more risk intelligent. Prior to delving into and proceeding through the documented ERM process, members of the board of directors and senior management should work to understand the major concepts, definitions, and objectives of ERM. This will facilitate education of the entire organization, effective board of director oversight, and provide an invaluable basis for execution of this initiative. Any organization that does not seek to educate itself in this way prior to commencing the ERM process would be severely handicapped. The entity is also at risk for failure or, at minimum, may not realize maximum benefit.

- *Incorporate risk into strategy.* Ideally an entity, led by its board of directors, should seek to embed risk management into the core business processes and structure of the organization. This is a long-term progression that begins with the risk education process referred to previously. It then involves ensuring that entity strategy and objective definition as well as any associated discussions and documentation include the consideration of risk. For example, companies may consider incorporating a discussion about risk—"What can go wrong?"—into the planning and budgeting processes. Any proposed strategic initiative deliberations should include an analysis of risks.
- *Define/determine risk appetite early.* It is vitally important that an organization consider, discuss, and define its risk appetite. The entity should take steps very early during the initial risk management program development process to ensure that the board of directors and management are clear and in agreement regarding the level of risk the organization is willing to take related to both specific incidents/events and the entity as a whole. In many cases, risk appetite is evidenced, although not specifically by name or definition, in company policies that outline things such as authorities and/or approval limits. Risk appetite determination will help facilitate critical discussions throughout the ERM program development process, including risk mitigation planning.
- *Consider building the ERM program in phases.* Many organizations are hesitant to embark on an ERM initiative because of the perceptions that risk management is highly complex, costly to implement, and requires extensive expertise and resources. Companies often are overwhelmed with the task of a full ERM implementation. They believe that risk management is an all-or-nothing proposition. This is not the case. Many organizations

have implemented a successful risk management program using a phased approach. This affords the entity the opportunity to achieve short-term success. In addition, members will further educate themselves regarding risk management and will be able to apply that knowledge and expertise during future implementation phases. Also, the organization can customize the remaining phases of the program to realize the most efficient implementation and maximum benefit for it. Success has been achieved by following the process outlined in the subsequent paragraphs.

- *Focus initially on a few agreed-on high risks.* If an entity chooses to adopt the phased implementation approach referred to previously, the organization should focus initially on a small group of identified high risks associated with the entity's documented strategic objectives. Another option is to focus on one category of risk. (Examples of risk categories are provided in Chapter 3.) Management can navigate through all steps of the risk management process for these identified risks. Doing so will help to build the foundation for a robust, holistic ERM program.
- *Use initial work as a platform for expanding the ERM initiative.* An entity should capitalize on the initial risk management work it performs and use that foundation as the platform for future initiative phases. The subsequent phase may include organization consideration of another single risk category, or it may choose a high-risk area or decide to remain at the overall broader strategic objective risk level.
- *Develop a monitoring process early on.* Risk management is a continuous evolution. Therefore, it is important that management develop an effective monitoring process that provides all appropriate groups and individuals, including the board of directors, with the necessary information to perform their risk management responsibilities. An ERM program will not be effective if it is designed and implemented but not monitored after initial completion.

In addition to the concepts listed, each organization must consider its culture and individual circumstances in determining the best ERM implementation approach.

SUMMARY

The increased focus and pressure on organizations to manage risk warrants management and board of director attention and support for the risk

management process. An effective risk management program can be implemented cost effectively. The initiative does not require a significant amount of time or resources (internal or external). There is a sufficient amount of guidance available to enable an entity to design and implement an ERM program that adds value to the organization and allows management to proactively make the best choices and decisions for the company.

NOTES

1 Sarah Johnson, "SEC Pushes Companies for More Risk Information," *CFO Magazine*, August 2, 2010, www.CFO.com
2 Kate O'Sullivan, "A Risk Top 10 for 2010," *CFO Magazine*, January 12, 2010, www.CFO.com